Strategy and working methods of Software security testing techniques

Mubarak Elamin Elmubarak Daleel

***Abstract*— We will speak in this search for software testing, which is an activity designed to assess the ability of the program and must ensure that the desired result is also a way to reduce errors and selection of technologies to develop the software and how to enhance the quality of the software and will discuss security software testing in order to verify the implementation of a safe product and reduce security vulnerabilities and security testing to find the weaknesses and keep the final product of malicious users.**

***Index Terms*—Software Testing, , Testing Technique, Software Testing Techniques.**

I. INTRODUCTION

Our society is now needed to the software because it depends on a lot of business activities and vital functions such as banking, telecommunications, aviation and control of hazardous substances when traveling This is a total reliance on software makes it a high-value target for in order to achieve financial gain or a military and political features to meet the needs of those who have Want exploitation or sabotage these activities And also there are defects of the software makes it a target for attackers and also can cause to operate these programs incorrectly and unexpected and there are a number of flaws that can be exploited deliberately by attackers to subvert the way it works program which makes it unreliable, or to sabotage the ability to work, making it un trusted .

The old software testing in the history of digital computers and software testing is an important means to evaluate the program to determine its quality and also require more time and effort for systems that require higher reliability levels, but is considered an important part of software engineering, which is working to accelerate the implementation and high process also Percentage of test and high amounts of time maintenance and upgrading of existing systems and there will be a large amount of tests to check for a change, despite the progress in road and verification techniques are also considered system has to be verified before it is used and is a software testing is an effective means to ensure the quality of the software system to check it before using it as well as one of the most programs a complex software engineering and software testing is considered one of the most interesting areas that have the level of research within computer science it is likely to become more important in the future .

Security software has also been tested, regardless of the functionality that the program is implemented and this task in assessing the safety and behavior characteristics of this program as a way interaction with other entities and the method of interaction with each other .

It is necessary to rely on software testing in order to verify that the programs that have been built to meet these specifications and to the inability to have the client in order to make it sure to be offered to the customer is a solution appropriate for programs go for testing and testing ensures that you get the result at the end and check whether there was nothing wrong with the system and that can make the program unusable by the client problems and this also helps to provide the prevention of errors in software engineering system .

II. THE HISTORY OF TESTING TECHNIQUES

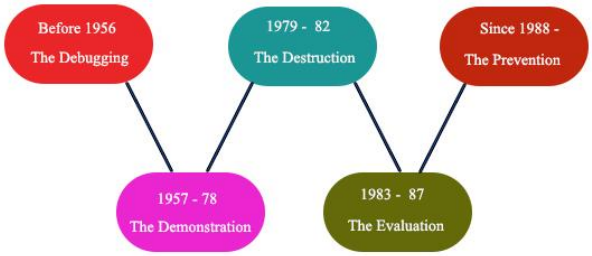
1 . Before 1956: The Debugging - Oriented Period – Testing was not separated from debugging

2 - 1957 - 78: The Demonstration-Oriented Period – Testing to make sure that the software satisfies its specification

3 – 1979 - 82: The Destruction-Oriented Period – Testing to detect implementation faults

4 – 1983 - 87: The Evaluation-Oriented Period – Testing to detect faults in requirements and design as well as in implementation

5 - Since 1988: The Prevention-Oriented Period – Testing to prevent faults in requirements, design, and implementation .



The History of Testing Techniques

" Fig " (1) : The History Of Testing Techniques

III. APPROACH

1 . Testing principles :

We will recognize the test principles to be followed in the style of work are as follows

1. Software testing is a process of implementation of a specific program with a view to finding errors and we must discover mistakes to make the testing process more efficient

2. Start software testing process early helps to identify errors in the early stages of development and reduces errors found in advanced stages

3. The test must be in the context of the test depends on getting different points of time

4. General Plan test determines the scale example of test strategic objectives and test schedule and test environment and other levels are applied methods and certain techniques are used and should be an alternative plan to meet the needs of the organization and efficient customer status
5. You must specify the test case and how to effectively test design even within which to measure the results of the test
6. Test carried out according to the correct input and we have a system of input conditions invalid and unexpected test
7. The test of several different people on different address from someone else's experience level before so you must be a different test using multiple technologies on a different level
8. End of the test must be to reach a certain result try to reduce the level of risk or failure
.

2 . Types of Testing :

This section describes the different types of testing that may be used to test a software

2 . 1 . Manual Testing .

Manual testing Is a manual software testing without the use of any use or to, or script In this type in this test depends on the role of the end user and tests to identify any unexpected behavior. There are different stages for manual testing such as unit testing, integration testing, system testing, and user acceptance testing .

2 . 2 . Automated Testing :

Automation testing, Automatic test also known name here and write scripts and uses another program to test the product of this process is used on manual operation are also used to re-test scenarios that have been implemented manually frequently and remarkably quickly

3 . Software Testing methods :

There are different methods that can be used for software testing.

3. 1 . Black-Box Testing

Black box testing is based on the analysis part of the software without reference to the inner workings of the objective test is the extent of the product prepared the requirements for publication agree and test the black box does not have an internal structure of the system because it check by the system is to make sure that input is accepted properly and are output production correctly in black box testing is to maintain the integrity of the final product and maintain the integrity of external information and we will review some of the different types of black-box testing methods are as follows :-

a) Equivalent Partitioning
b) Boundary value Analysis
c) Cause-Effect Graphing Techniques
d) Comparison Testing

Advantages :

1.It is completely appropriate and commensurate with the large slide code
2. You cannot access code
3. Clearly is the separation of the roles of both the developer and user perspective
4. Be large numbers of skill tests and tests the application and have the knowledge of the implementation of the programming language or operating systems

Disadvantages

1. Coverage is limited because a certain number of scenarios have already been implemented
2. The test is effective, because the test has a limited knowledge through the application
3. Coverage is blind because the test can not be aimed at specific code segments
4. Be a difficult test case design .

Black Box Testing

" Fig " (2) : . Black-Box Testing

3 . 2 . White box testing .

Testing white box have an effective ability to detect and solve problems because when you discover mistakes possible to cause trouble and also there are several names to test the White Fund, a glass test or open-box testing and this test needs to know the internal workings of the programmed operations and there are some different types test of the white box techniques as follows :-

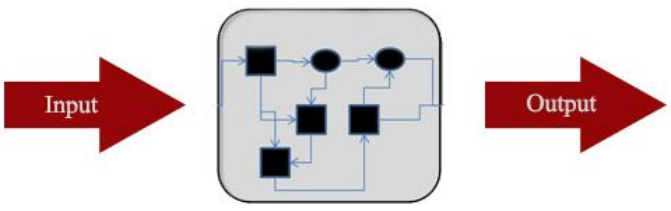
1) Basis Path Testing
2) Loop Testing
3) Control Structure Testing

Advantages

1. This test have knowledge of the source code and it becomes very easy to see what kind of data that can help in the effective application
2. Is optimizing the code
3. The removal of extra lines of code that can bring a lot of flaws
4. This is achieved maximum coverage while writing test scenario
5. Internal data structures exercise regime to maintain her health
6. The disclosure of hidden icons

Disadvantages

1. Be no need to test the white box to test the skilled and be an increase in costs
2. It is impossible to look at every angle and every corner to see the hidden errors that may cause problems
3. It requires the preservation of the white box testing the use of specialized tools such as code analysis or debugging tools



White Box Testing

" Fig " (3) : . white Box Testing

3 . 3 . Grey Box Testing

Gray box test depends on the methodology used software testing software testing this methodology applications have language-independent and this methodology relies heavily on the use of the host debugger to validate the program under test Recent studies have confirmed that the method of gray test box can be applied in real time using the software Primary law

Advantages

1.It offers the benefits of a joint between the black box testing and white box testing

2. It does not depend on the source code, but rather depends on the functional specifications

3. It can test the gray box excellent scenarios especially about the protocols and the type of traded data design and be based on the limited information available

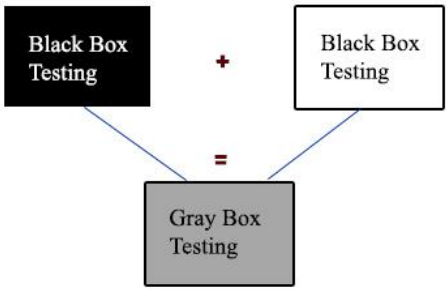
4. This test is according to the user's perspective, not the designer

Disadvantages

1. Lack of access to the source code and have the ability to go to code coverage and testing limited

2. Tests be redundant if the program is designed to run optionally

3. Each input test because it is a time thing for taking some time because many of the paths are untested program



" Fig " (4) : Grey Box Testing

4 . Software Testing Level :

There are four different software testing strategies :

4 . 1 . Unit testing .

Unit testing is a one of the test levels, which go together to make the system test in the big picture, as well as unit testing called Test square white category, which assesses code, which has to be implemented instead of corresponding to some of the requirements that are implemented this type of testing by developers before assessing that is preparing to deliver more than a team to carry out the official test cases and unit testing is performed by the developers on individual units of the areas allocated to the source code and is used to test data in order to ensure quality individual units of the areas allocated to the source code and is used to test data in order to ensure quality .

Benefits of Unit Testing :

1. The unit test level is very effective

2. Be in a much greater reliability of the extended test of the system resources to it tends to detect bugs

3. Be able to test parts of the project without waiting for the other parts to be available

4. Be able to detect and remove defects much lower cost compared with other stages of testing

5. Be able to benefit from a number of official testing techniques available

Limitations of Unit Testing

You cannot catch every mistake is in the application because it is impossible all the tracks evaluation of the application software and be the same thing with the unit test and there is a limit to the number of scenarios and test data in the application, which can be used to verify the source code and that after exhausting all options are not there but to stop testing and integrating code segment with other units .

4 . 2. Integration testing

Integration testing is defined as the testing of combined parts of an application to determine if they function correctly. Integration testing can be done in two ways: Bottom-up integration testing and Top-down integration testing.

4 . 2 . 1. Top down Integration

Integration from top to bottom is a test of a gradual approach to building the structure of the program are integrated units by moving to the bottom through a certain structure and be starting from the main console, and then be integrated into the units to the main control unit in the temple either by first depth or breadth In this first test units are tested at the highest level first gradually and then test units are at a low level thereafter

4 . 2 . 2 . Bottom up Integration

Begin this test with the unit test followed by tests gradually on the sets at a higher level are called units or construction of bottom-up integration testing begins construction with units offspring because it is the integration of components from the bottom to the top and there is a treatment for all certain levels and get rid of the seed .

4 . 3 . System testing

System testing of hardware and software is a test being full integrated system to evaluate the optimum system with the specified requirements and is testing the system within the scope of testing black box and therefore does not need to know the interior design of the law or logic is testing the system a series of different tests the existing system in the entire practice on the computer and each test has a different purpose and is verified that the system has been integrated elements properly and perform assigned tasks . Some of Different types of system testing are as follows:-

1. Recovery testing
2. Security testing
3. Graphical user interface testing
4. Compatibility testing

4 . Acceptance testing

Acceptance testing is a type of tests conducted in order to verify that the product has been developed according to the required standards and protects all the internal requirements by the customers and are the kind of tests by a user or customer, where the product is externally from one party to develop and fall admission test of Within the framework of the black box testing methodology where the user is not interested so much work in the inside work but be interested in overall system performance assessment and the comparison with the specific requirements of them is acceptance testing is one of the most important experiences by the user before they are delivered at the end of the day the system or are It delivered the final product acceptance testing is also known as the User Acceptance Testing. Here we can say that the acceptance test is the most important type of tests because he

is being undertaken by the quality assurance team, which measures whether the applicant fulfills the requirements and desired specifications and meets business requirements

Software Testing Level

" Fig " (5) : Software Testing Level

5 . security testing

Security Test is a test is the only system to assess the presence of security vulnerabilities in the system, a specialized assessment system tests with a range of specialized tools, and security testing is basically a type of software tests in order to verify the product whether or not it checks whether this application is prone attacks and verification of system penetration process or access to the application without permission, a process to challenge the existence of an information system protects data and maintains its function as intended . The objective of security testing is to identify the threats in the system and measure the weaknesses and potential strengths as it also helps to detect potential security risks in the system and help developers in identifying these problems by coding .

5 . 1 - objectives of Security Testing

The greatest security defects are not so easily discovered to be a security test, which is determined by the defects beyond recognition and is also a test to make sure that the program is strong enough even if subjected to a malicious attack will be steadfast and not affected and this is The objectives can be:

1. must be done to provide adequate attention to the lack of exposure to security risks
2. It must be to provide a mechanism to define and enforce access to the system
3. It must be supplied sufficient expertise to perform adequate security test
4. it must be conducted checks to ensure proper functioning of the system

5 . 2 - Methods of Security Testing :

1. Functional security testing:

The program is supposed to act in accordance with certain requirements and be limited expect to prove these requirements Limited complete satisfaction at an acceptable level

2 . Risk-based security testing:

This method is done on steps the first step is a test on the basis of risk which is about determining the potential risks of these risks and losses it tries to develop immunity against the potential risks that have been identified through risk analysis and testing on the basis of risk addresses the political requirements that assume that the program does not work the tests derive political requirements through risk analysis are covered in general on the high-level risks that have been identified through the design process, but also address the risk at a low level of the program itself

5 . 3 Types of Security Testing :

5 .3 .1.Vulnerability Scan

After the discovery phase known security issues using automated tools fit with the circumstances weaknesses risk level is set by a tool that can not be verified and could be completed on the basis of the preparation of the survey that is looking to remove some common false positives using forged papers Accreditation

5. 3 . 2 . Vulnerability assessments

The vulnerability assessment via a comprehensive survey of security issues using a combination of automated tools and techniques of manual assessment and when assessing vulnerabilities and security testing to make sure there is actually exploited and this means they do not carry out an attack For but are making the effort to make sure that there is a possible attack only be evaluated vulnerability on time less than penetration tests, but sometimes do not conclusively prove that the attacks are possible and have the potential impact of a weak attack .

5. 3 . 3. Security Assessment

The vulnerability evaluation for manual check to confirm exposure but does not include the exploitation of vulnerabilities to gain more access and is verified in the form of access to the system to confirm the settings system include examination of records and system responses and error messages and looks Security Assessment for wide coverage of the system under test, but not the depth of exposure this weakness .

5. 3 . 4 . Penetration tests

Penetration testing is a vulnerability assessment, but the test is actually an exploit weaknesses and the goal is to simulate a real striker who can break into the system and data theft, and many security teams use them as a means to prove the real danger is not to challenge the security issues and measure the vulnerability and penetration tests, which be more accurate because they have fewer false positives, but take a longer time because of the increased time and penetration tests are considered the most dangerous vulnerability assessments because they are more susceptible to influence negatively on the availability of data and system integrity .

5 . 3 .5 . Security Audit

Is a scrutiny of risk, control and compliance with specific issue, which is characterized by a narrow range can be for this kind of participation to take advantage of the previous methods, which explained such vulnerabilities and assess security and penetration testing to assess

5. 3. 6 . Security Review

Here you will be checked that the industry and internal security standards were applied to the components of the system or product and usually this process is done through the gap analysis is used to review the law through a review of design documents and drawings of architectural and this activity does not use any of the previous methods, such as weaknesses and assess the security and test evaluation penetration and security Audit

6 . Security testing approach :

In order to conduct security tests and be useful for web applications , the security tester should have good knowledge of the HTTP protocol. It is important to have an understanding of how the client (browser) and the server communicate using HTTP. Additionally, the tester should at least know the basics of SQL injection and XSS .

6 . 1. Password cracking:

Launched safety test Web applications by password cracking stage in order to allow for entry into special areas of application because one can guess a user name and password, or use some of the tools for cracking the password is also available next to the password lists of usernames and passwords most commonly used passwords and if Web application has not been applied a complex password and it may take a very long time to eliminate the user name and password, and if the store the user name and password in the cookies without encryption attacker can use different ways to steal the cookies are then steal information stored in cookies such as the name of the file user and password

6 . 2. URL manipulation through HTTP GET methods:

Security testing must be done to see if the application is passed important information to the query, this only occurs when you use the application HTTP method to pass information between client and server can be tested adjust the value of information in the query string to check if the server accepts it or not. Over HTTP is a request user information to the server for honest it pass or bring data, an attacker can manipulate all the variables is a variable passed this request to the server in order to obtain the required by the information or corrupting data in such circumstances, any behavior is considered unusual by the application or web server is the gateway for attackers to gain access to the application

6. 3. SQL Injection:

will be checked from the SQL injection is a single quote (') in any text should be rejected by the application for if there was an error in the database, it means, it means that the user name inserted in some of the query that has been implemented by the application is injection attacks SQL is very critical, because an attacker can get vital information from the server database to check entry points in your web application and find out code from your database because it is directly execute SQL queries for the computer to the database through the user acceptance of some input

If the introduction of user data in SQL queries to the database can be the attacker inject SQL database or part of the data as inputs to the user in order to extract vital information from the database if successful attacker to disable the application, it is wrong to query SQL that appear on the browser and the attacker can get the information they are looking for and should be handled with special characters from the user input

4. Cross Site Scripting (XSS):

The tester should additionally check the web application for XSS (Cross site scripting). Any HTML e.g. <HTML> or any script e.g. <SCRIPT> should not be accepted by the application.

Attacker can use this method to execute malicious script or URL on victim's browser. Using cross-site scripting, attacker can use scripts like JavaScript to steal user cookies and information stored in the cookies.

Attacker can easily pass some malicious input or <script> as a '&query' parameter which can explore important user/server data on browser.

Must be taken into account during the security test must be very careful not to modify any of the following

1. Application or server configurations
2. Services that run on server
3. List of user data, which was hosted by the client or in addition to the security test should be avoided on the production system

The purpose of the test is to discover security weaknesses in web applications so that developers can remove the weaknesses of this application and also make a secure application on the Internet

IV. RESULTS

Will speak here about the software testing in detail, we desperately need it and its objectives and principles, as well as software testing be less strict than some people think about the main reason is that we desperately need it to identify best practices, methodologies and standards homosexual to test the software in order to perform software testing effectively and efficiently must be familiar targets basic software concepts . Software testing is a process that can be planned and identify an important approach and can hold her design and conduct strategy and are evaluating the results on the basis of specific expectations and thereby reach a successful outcome when a line particular van is detected correction process leading to remove the error and the purpose of the correction process is to determine the place and repair the offending code responsible for the error correction usually done through three activities in the field of the development of the first software is during the encoding process and the second is when translated programmed specific design into executable code and also through this process is where the programmer to write code can lead to defects that need to explore before moving to the next stage, which has to be the solution before moving on .

We will talk about the security of software that include penetration testing, which stresses the analysis and design of the symbol and the investigation also software behavior and verifying that the program complies with the security requirements of the process of testing whether or not there is the security test that is according to plan and security measures test establishes the obligation of the program with the security requirements and security testing focuses on identifying weak points and software to identify unexpected situations that can cause failure of the program, which will cause the violation of security requirements are often limited to the security test requirements of the program, which it describes the security elements

REFERENCES :

[1] 1 . Software testing-Brief introduction to security testing by Nilesh Parekh published on 14-07-2006
[2] *available at http://www.buzzle.com/editorial/7-14- 2006-102344.asp*
[3] 2 . Introduction to software testing available at *http://www.onestoptetsing.com/introduction/*
[4] 3 . S.M.K Quadri and Sheikh Umar Farooq,"Software Testing-Goals,Principles and Limitations," *International Journal of Computer Applications, Volume 6-No.9,September 2010.*
[5] 4 . Jovanovic and Irena,"*Software Testing Methods and Techniques," May 26,2008.*
[6] 5. Software testing techniques available at *http://pesona.mmu.edu.my/~wruslan/SE3/Readings/*

[7] *GB1/pdf/ch14-GB1*
[8] 6 . Mohd. Ehmer Khan,"Different Forms of Software Testing Techniques for Finding Errors*,"IJCSI International Journal of Computer Science Issues,Vol. 7, Issue 3, No 1, May 2010.*
[9] 7. Security testing-wikipedia the free encyclopedia available at *http://en.wikipedia.org/wiki/securitytetsing*.
[10] 8 . Thompson, H., Why Security Testing is Hard, *IEEE Security and Privacy, July/Aug 2003, pp. 83-86.*
[11] 9 . Whittaker, J., How to Break Software Security, *Addison Wesley, 2004.*
[12] 10 . G. McGraw, "Software Security," *IEEE Security & Privacy, vol. 2, no. 2, 2004, pp. 80–83.*
[13] 11 . J. Whittaker and H. Thompson, *How to Break Software Security, Addison-Wesley, 2003*.
[14] 12. Kelley, Diana. "Black Box and White Box Testing: Which Is Best?" Search
[15] *Security.com. 18 Nov. 2009. Web.*
[16] 13 . PROTOS - security testing of protocol implementations. [Online]. Available: *http://www.ee.oulu.fi/research/ouspg/protos/*
[17] 14 . T.R. Dean, G.S.N. Knight, "Applying Software Transformation Techniques to Security Testing", International Workshop on Software Evolution and Transformation, Delft, *Netherlands, November 2004, pp. 49-52. [Online]. Available*:
[18] 15 . Girish Janardhanudu. White Box Testing *(https://buildsecurityin.us cert.gov/bsi/articles/best-practices/white-box/259-BSI.html).*
[19] 16 . Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, and Nancy R. Mead. *Software* Security Engineering: A Guide for Project Managers. *Upper Saddle River, N.J.: Addison-Wesley. 2008.*
[20] 17. Kiezun A, Guo P, Jayaraman K, Ernst M. Automatic creation of SQL injection and cross-site scripting attacks. *In Proceedings of the International Conference on Software Engineering, May 2009; 199–209.*
[21] 18 . Wang L, Wong W, Xu D. A threat model driven approach for security testing. *In The 3rd International Workshop on Software Engineering for Secure Systems, May 2007.*
[22] 19. Wysopal C, Nelson L, Zovi DD, Dustin E. The Art of Software Security Testing: *Identifying Software Security Flaws (Symantec Press). Addison-Wesley Professional: Boston, MA, 2006.*
[23] 20. Shahriar H, Zulkernine M. MUSIC: Mutation-based SQL injection vulnerability checking. *In Proceedings of the 8th International Conference On Quality Software, Aug 2008; 77–86.*

Mubarak Elamin Elmubarak Daleel, Department Of Information System , University Of Jeddah Faculty Of Computer& Information Technology , KSA Department Of computer science , AlzaeimAlazhari University Faculty Of Computer science &Information Technology , sudan